Electronic Version
Stylesheet Version v1.1.1

Description

CRYPTO-SYSTEM WITH AN INVERSE KEY EVALUATION CIRCUIT

BACKGROUND OF INVENTION

[0001] 1. Field of the Invention

[0002] The invention relates to a crypto-system, and more particularly, to a crypto-systemwith an inverse key evaluation circuit and a related decryption method for reducing use of random access memory (RAM).

[0003] 2. Description of the Prior Art

[0004] A major difference between a wireless LAN and a normal fixed LAN is that the wireless LAN transmits data by radio, but the later transmits data by cables or optical fibers. Since radio can be intercepted more easily, the security of data is a major focus of wireless LAN. For example, IEEE provides 802.11i as a standard to enhance the data security of wireless LAN. In fact, the concept of using cryptography to provide networks with better security protection

can be applied to each kind of network transmission.

[0005] Among those, the data encryption standard (DES) using a 56-bit key is the most famous and widely used. However, as electronic technology develops and processing speeds of computers improve, concepts and experiments involving the design of special hardware or the organization of many computers for solving the data encryption standard have been increasing of late. This leads to lower the security of systems that use the DES as an algorithmic mechanism.

[0006] In Oct 2000, NIST declared that the Rijndael algorithm was chosen for use in a new standard -- Advanced Encryption Standard (AES), which became a data encryption standard of the United States in 2001 and aimed to gradually replace previous data encryption standards. The Rijndael algorithm and the AES based thereon are shown in the literature of "Rijndael, the advanced encryption standard" disclosed by J. Daemen and V. Rijmen in *Dr. Dobb's Journal* 2001.

[0007] The AES is a block cipher/decipher algorithm. It plays a central role for realizing the network security of the IEEE 802.11i standard. All security modes are extended applications based on the AES. In current cryptography tech-

nology, which is grouped according to key types, the AES is regarded as a symmetric encryption system because its encryption operations and decryption operations are based on the same key.

[0008] Due to this property, the security of a symmetric encryption system depends on two things. First, the enciphering algorithm must be powerful enough to make it impossible in practice to obtain deciphered information only according to the enciphered texts. Secondly, the security of the encryption is dependent on the security of the keys but not on the security of the encryption/decryption algorithm. As a result, the secret of the keys becomes more important. In US Patent No. 5,539,827,"Device and method for data encryption" disclosed by Liu etc., a user could utilize a key to determine the encryption/decryption intensity and increase the secret of the encryption process. In US Patent No. 6,192,129,"Method and apparatus for advanced byte-oriented symmetric key block cipher with variable length key and block" and US Patent No. 6,243,470, "Method and apparatus for advanced symmetric key block cipher with variable length key and block" disclosed by Coppersmith etc., encryption/decryption algorithms similar to the AES are also disclosed, and keys

with variable lengths determined by users are also provided to increase the complexity of the encryption process. The plain text in the AES is fixed to 128-bits and the key is also 128-bits.

[0009] Please refer to Fig.1, which is a functional block diagram of a conventional crypto-system 10 qualified under the AES. As shown in Fig.1, each round in the AES is composed of four reversible converting layers which are: a key addition layer 12, a byte substitution layer 14, a shift row layer 16, and a mix column layer 18. A controlling module 20 is used to control the evaluation in each round.

[0010] The round evaluations through the four layers will be repeated 10 times in total, wherein different keys are used in each round evaluation. These different keys are generated by a key scheduling module 22 for increasing the disorder degree of the encoded data. Thus, an encryption process qualified under the AES with 128-bit keys can be performed as shown in Fig.1. First, a 128-bit key, which is a first key or so-called original key, is expanded to generate another 10 128-bit keys. Each newly generated key is used in a different round evaluation to perform an encryption/decryption operation for a document. As a result, the document will experience encryption/decryption op-

erations 11 times according to eleven 128-bit keys, one original key and 10 keys derived from the original.

[0011] In the implementation of the AES, the key scheduling module performs an important algorithm. As previously mentioned, the purpose of the key scheduling module is providing a new key according to the key given by the upper layer, in which the new key is totally different from the previous key. In other words, a plurality of related but totally different keys are generated to ensure the encryption method based on the keys can make enciphered data extremely different from the original data.

[0012] Please refer to Fig.1. The AES structure further comprises a read only memory (ROM) 24 for storing algorithms corresponding to the plurality of encryption/decryption operations and related application programs. Furthermore, the prior art technology has a random access memory (RAM) 26 for storing temporary operating variables i.e. the generated keys, from which a proper key is picked in each round evaluation.

[0013] In evaluating the performance of an algorithm, bigger programs and tables, which occupy a larger area of the ROM 24, or more temporary operating variables such as the generated keys, which occupy a larger area of the RAM

26, usually improve the operation speed of encryption/decryption. However, increasing the occupied area of memory increases the cost. In addition, the more generated keys stored in the RAM 26, the bigger the delay in the data access time of the receiver, which leads to lower system performance. As mentioned above, the RAM 26 must store eleven 128-bit keys comprising the original key and its 10 derivatives, so a certain amount of space and cost are necessary.

SUMMARY OF INVENTION

[0014] It is therefore a primary objective of the claimed invention to provide a crypto-system with an inverse key evaluation circuit and a related method to reduce the use of memories to solve the aforementioned problems.

[0015] According to the claimed invention, an inverse key evaluation circuit and a related method applied to a crypto-system are provided to reduce the use of the RAM and also avoid the time delay associated with the receiver accessing the data in the RAM. The crypto-system in the claimed invention performs the encryption operation and the decryption operation with two different modules. The encryption operation uses a ROM-based method to increase the operating speed. The decryption operation uses an in-

verse key evaluation circuit and a related encryption method. Both the encryption and decryption operations use the same key generating module to keep the hardware qualified under the AES. By doing so, the circuit operating speed is not decreased, and no additional circuits are required.

[0016] The claimed invention provides an inverse key evaluation circuit applied to a crypto-system comprising a key receiving module comprising an N-bit register, which comprises m groups of registers for receiving an N-bit key. The N-bit key comprises m groups of keys, which are stored in the m group of registers respectively. Both N and m are power-of-two integers larger than two.

[0017] The inverse key evaluation circuit further comprises an inverse key evaluation module comprising an m XOR logic gates and a digital data processing module for inverse evaluation to sequentially generate a plurality of pre-keys according to the keys received by the key-receiving module. The keys stored in the N-bit register are sequentiallyreplaced by the pre-keys, which are obtained by utilizing the inverse key evaluation module to process the keys one at a time.

[0018] The claimed invention also provides a decryption method

to decrypt an N-bit enciphered text string into a corresponding N-bit plain text string wherein N is a power-of-two integer larger than two. The decryption method comprises following steps: providing a key and the enciphered text string, using an inverse key evaluation module to generate a plurality of pre-keys according to the key, and utilizing the key and the sequentially-generated pre-keys to perform a plurality of corresponding decryption operations to decrypt the enciphered text string into the plain text string.

[0019] Furthermore, the claimed invention also provides a crypto-system for performing a plurality of encryption operations and decryption operations. The crypto-system comprises a key generating module for providing a plurality of keys. The key generating module comprises a forward key evaluating circuit and an inverse key evaluating circuit. The forward key generates a plurality of post-keys according to the original key. The inverse key evaluating circuit uses the last post-key to generate a plurality of pre-keys the last being the original key.

[0020] The crypto-system further comprises an encryption module and a decryption module both electrically connected to the key generating module. The encryption module is

used for performing a plurality of encryption operations that encrypt a plain text string into a corresponding enciphered text string according to the original key and the sequential post-keys generated by the forward key evaluation circuit. The decryption module is used for performing a plurality of decryption operations that decrypt an enciphered text string into a corresponding plain text string according to the original key and the sequential pre-keys generated by the inverse key evaluation circuit.

[0021] It is an advantage of the claimed invention that the crypto-system and the related method can reduce the use of the memories to solve the aforementioned problems.

[0022] These and other objectives of the present invention will no doubt become obvious to those of ordinary skill in the art after reading the following detailed description of the preferred embodiment, which is illustrated in the various figures and drawings.

Brief Description of Drawings

[0023] Fig.1 is a functional block diagram of a crypto-system qualified under the advance encryption standard (AES) in the prior art.

[0024] Fig.2 is a functional block diagram of an inverse key evaluation circuit according to an embodiment of the present

invention.

[0025] Fig. 3 is a functional block diagram of inverse key evaluation circuit according to the embodiment of Fig.2.

[0026] Fig.4 is a flow chart of a decryption method according to the present invention.

[0027] Fig.5 is a functional block diagram of a crypto-system of the present invention.

[0028] Fig.6 is a functional block diagram of an inverse key evaluation circuit according to an embodiment of Fig.5.

DETAILED DESCRIPTION

[0029] The technological feature of the present invention is based on the AES, and the purpose of the present invention is to implement the AES with hardware offering the best performance. In the present invention, an inverse key evaluation circuit is first disclosed for evaluating a plurality of related pre-keys of a key so that the use of the RAM can be reduced. By using some technological features in the prior art shown in Fig.1 of a crypto-system, during encryption using an original key, 10 groups of post-keys are calculated. In the decryption, the order of the needed keys is opposite to that of encryption. In other words, if the sequence order of evaluated keys in the encryption is key 0 (the original key), key 1, key 2, key 3, ... and key 10,

the sequence order of needed keys in decryption is key 10, key 9, key 8, ... and key 0 (the original key).

[0030] Please refer to Fig.2, which is a functional block diagram of an inverse key evaluation circuit 32 according to an embodiment of the present invention. The inverse key evaluation circuit 32 comprises a key receiving module 34 and an inverse key evaluation module 36. The key receiving module 34 comprises an N-bit register 38, which comprises m groups of registers for receiving a N-bit key. The N-bit key can be divided into m groups of keys. The m groups of keys are stored in the m groups of registers respectively. N and m are both power-of-two integers larger than two.

[0031] In the present embodiment, N is 128 due to the rule of the AES and m is set to 4 due to the algorithm. However, the value of N and M can be adjusted in advance according to the situation in practice. The inverse key evaluation module 36 comprises m XOR logic gates 40. In other words, the number of the XOR logic gates corresponds to the number of m keys in a group with each XOR logic gate performing an XOR operation on two of the keys from the m groups of keys. The inverse key evaluation module 36 further comprises a digital data processing module 42

electrically connected to the m XOR logic gates 40 for inversely evaluating the keys received by the key receiving module 34 to generate a corresponding plurality of pre-keys.

[0032] Similar to the aforementioned conventional technology, the process repeats for 10 times to generate 10 pre-keys in sequence. If the 128-bit key is called key 10, the pre-keys are key 9, key 8, ... and key 0 in sequence. Notice that the keys stored in the N-bit register 38 of the key receiving module 34 are replaced sequentially by the pre-keys obtained by utilizing the inverse key evaluation module 36, which processes the keys one at a time. In other words, according to the feature of the present invention, only one N-bit register 38 a 128-bit register - is required for storing the generated keys wherein the register can be realized by a RAM in practice. Compared with the prior art technology, this kind of inverse key evaluation mechanism is not available, meaning that the RAM must store all the keys comprising the original key and the keys generated from the original key for a total of eleven 128-bit keys. As a result, the inverse key evaluation circuit can effectively reduce the space and cost of the RAM circuit.

[0033] Please refer to Fig.3, which is a detailed functional block

diagram of the inverse key evaluation circuit 32 in Fig.2. The digital data processing module 42, which is electrically connected to four XOR gates 40, comprises a byte rotator 43, a byte substituter 45, and a byte distributor 47. The byte rotator 43 is used to reverse the order of the bytes in the input key. The byte substituter 45 is electrically connected to the byte rotator 43 for replacing a plurality of bytes in the key with a plurality of predetermined bytes. The byte distributor 47 generates a distribution value according to a predetermined distribution table and performs XOR operations with the plurality of bytes in the key.

[0034] After being processed once by the four XOR logic gates 40 and the digital data processing module 42 of the inverse key evaluation circuit 32, the newly obtained pre-key is stored in a register 48 in the present embodiment. The register 48, which is electrically connected to the inverse key evaluation module 36, works in the same manner as the 128-bit register 38 in the key receiving module 34 shown in Fig.2 and Fig.3. The key stored in the register 48 is replaced each time by each newly obtained pre-key, which is the result of an inverse evaluation of the key. As a result, the register 48 only needs 128 bits for storing

the key.

[0035] In the present embodiment of the present invention, two registers, which are 128-bit register 38 in the key receiving module 34 and the additional register 48, are employed. A pre-key obtained after an inverse key evaluation is first stored in the additionally employed register 48. A key renewer is required to then copy pre-key into the 128-bit register 38. The key renewer 50, which is electrically connected to the 128-bit register 38 in the key receiving module 34 and the additional register 48, does so in response to a key renewing signal.

[0036] Since the theory of the inverse key evaluation circuit 32 in the present embodiment is based on the AES, the inverse key evaluation circuit 32 in the present embodiment can be applied to a wireless LAN, specifically to a decryption related method and apparatus. Please refer to Fig.4, which is a flow chart of a decryption method according to Fig.2 and Fig.3. The decryption method of the present invention is used to decrypt an N-bit enciphered text string into a corresponding N-bit plain text string. N is a power-of-two integer larger than two. According to the embodiments shown in Fig.2 and Fig.3, N is 128, meaning the enciphered text string and the plain text string are both

128-bit text strings. According to the AES, the key is also set to 128-bit. The decryption method comprising steps in following:

[0037] Step 100:Providing a key and an enciphered text string;

[0038] Step 101:Using the inverse key evaluation module 36 to generate a plurality of pre-keys from the key;

[0039] Step 102:Using a key register 48 to store the key and the plurality of pre-keys sequentially generated from the key;

[0040] Step 103:Using the key and the plurality of pre-keys, sequentially generated from the key, to perform a plurality of decryption operations to decrypt the enciphered text string to the plain text string.

[0041] In step 102, the key stored in the register 38 is continually replaced by the next sequential pre-key. The pre-keys are obtained one at a time by utilizing the inverse key evaluation module 36 to process the key stored in register 38. Thus, the register 48 only needs 128 bits because it only needs to store one key at a time. It is much different from the conventional RAM, which needs much space to store all 128-bit keys 11 in total.

[0042] All the aforementioned embodiments and methods are based on the feature of the inverse key evaluation circuit 32 in the present invention, which is using a last key to

generate a plurality of pre-keys thereof. As mentioned above, during decryption with a 128-bit key, which is called a last key, 10 groups of pre-keys are generated by the inverse key evaluation circuit 32. In encryption, the order of the needed keys is opposite to that of decryption i.e. a first key also known as an original key is used to generate 10 post keys with the last post key being the same as the last key used in decryption. Thus, not all keys are required to be stored since all the pre-keys can be generated if the last key is stored. This is the most important function of the inverse key evaluation circuit 32.

[0043] A functional block diagram of the crypto-system 60 in the present invention with the inverse key evaluation circuit 32 is shown in Fig.5. The crypto-system 60 comprises a key generating module 62, an encryption module 64, and a decryption module 66. The key generating module 62 can be used to evaluate or generate a plurality of keys, which are required in encryption and decryption. It also determines if the encryption module 64 or the decryption module 66 is working and transmits corresponding keys to the proper module.

[0044] The key generating module 62 further comprises a forward key evaluation circuit 70, an inverse key evaluation

module 72, which corresponds to the inverse key evaluation circuit 32 shown in Fig.2 and Fig.3, and a register 78. The forward key evaluation circuit 70 can generate a plurality of post-keys of an original key according to the original key until generating the last key. The inverse key evaluation circuit 72 can generate a plurality of pre-keys of the last post key according to the last post-key until generating the original key.

[0045] According to the AES, suppose that the order of evaluation of the forward key evaluation circuit 70 is key 0 (the original key), key 1, key 2, key 3, ... and key 10. Then the order of the evaluation of the inverse key evaluation circuit 72 is key 10, key 9, key 8, ... and key 0 (the original key). In addition, the register 78 in the key generating module 62 is used to store the original key (key 0). When the encryption module 64 wants to encrypt a plain text string to an enciphered text string, the forward key evaluation circuit 70 provides the original key (key 0) stored therein and the plurality of post-keys generated according to the original key to the encryption module 64 in sequence. During this time, the register 78 stores the last key (key 10) for provision to the decryption module 66 to decrypt the enciphered text string.

[0046] The reason why the register 78 is used to store the last key (key 10) is to save time. By saving the last key (key 10), additional time does not need to be spent by the forward key evaluation circuit 70 to evaluate the last key (key 10) whenever encrypted data is received. In other words, when the last key (key 10) is evaluated in encryption, it is stored in register 78. The last key can then be directly provided to the inverse key evaluation circuit 72 during decryption for processing instead of waiting for the forward key evaluation circuit 70 to evaluate the last key from the original key.

[0047] The encryption module 64 comprises an encryption circuit 65 electrically connected to the key generating module 62 for sequentially performing a plurality of corresponding encryption operations according to the original key (key 0) and the sequentially generated post-keys (key 1-10), which are provided by the forward key evaluation circuit, to encrypt a plain text string into a corresponding enciphered text string. These encryption operations are similar to the round evaluation shown in Fig.1. However, in this embodiment, the encryption module 64 with the encryption circuit 65 is an improved ROM-based encryption module 64 comprising a plurality of ROMs 74 for storing

the algorithm corresponding to the plurality of the encryption operations and the related application programs. Thus, the functions of each of the four reversible transfer layers can be replaced by the ROMs 74 which can operate faster with the programs and tables stored therein.

[0048] The decryption module 66 is also electrically connected to the key generating module 62 for sequentially performing a plurality of corresponding decryption operations according to the last post-key (key 10) and the sequentially generated pre-keys (key 9 to 0), which are provided by the inverse key evaluation circuit 72, to decrypt an enciphered text string into a corresponding plain text string. These decryption operations follow the structure of using a plurality of round operations for decryption, which is described in Fig.1. It means that a key addition layer 82, a byte substitute layer 84, a row shift layer 86, and a column mix layer 88 are used for performing the corresponding decryption operations to decrypt an enciphered text string into the original plain text string.

[0049] Note that the forward key evaluation circuit 70 of the key generating module 62 in the present embodiment is similar to the aforementioned key scheduling module 22 in the prior art. Please also note that the register 78 in the

present embodiment only needs to store the original key (key 0) and the last post-key (key 10). One could also have the register 78 only store the original key (key 0) if the inverse key evaluation circuit 72 further comprises an additional register for storing the last post-key (key 10). No matter which kind of circuit layout is set, the used memory can be reduced effectively in comparison with the prior art technology, which needs to store all keys (key 0 to key 10).

[0050] Please refer to Fig.6, which shows an embodiment of the inverse key evaluation circuit 72 in Fig.5, similar to the embodiment shown in Fig.2. It comprises a key renewer 90, a key receiving module 94, an inverse key evaluation module 96, and a register 98. The key receiving module is used for receiving and storing the last key (key 10). The inverse key evaluation circuit 96 is used to generate a plurality of pre-keys (key 9 to key 0) according to the last key (key 10) received by the key receiving module 94 until generating the original key (key 0). The register 98 is electrically connected to the inverse key evaluation module 96 for storing a pre-key, which is obtained through an inverse evaluation. In the same manner as mentioned earlier, the key stored in the register 98 is continually re-

placed by a newly generated pre-key, which is obtained from the inverse evaluation of the key.

[0051] When the crypto-system 60 in Fig.5 performs a system reset or replaces the old original key (key 0) with a new original key, an initialization process is performed to evaluate the last key (key 10) from the new original key (key 0) by the forward key evaluation circuit 70 in Fig.5. At that time, the key renewer 50 receives a key renewing signal to update the new last key (key 10) into the key receiving module 94. The key renewer 50 can then rewrite the pre-key, which is obtained through one inverse evaluation, from the register 98 to the key receiving module 94.

[0052] The crypto-system in the present invention performs the encryption and the decryption with two different modules. The encryption is performed in a ROM-based method to increase the calculation speed, and the decryption uses an inverse key evaluation circuit and its related algorithm to inversely evaluate the pre-keys sequentially. Only a small amount of memory is required for storing the initial key and the last key. As a result, the usage of the RAM can be reduced, so that the accessing data delay of the receiver can be avoided. Furthermore, the encryption and decryption in the crypto-system of the present invention both

use a common key generating module. As a result, the operation speed can remain fast, and no additional circuits are required to realize the hardware qualifications of the AES.

[0053] Those skilled in the art will readily observe that numerous modifications and alterations of the device may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.